IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Matter of the Application of: Luciano Fenizia et al.
Serial No.: 10/690,016 Confirmation No.: 4792
Filed: October 21, 2003
For: System and Method for Distributing a Media Content File Over a Network
Examiner: Brian P. Whipple Group Art Unit: 2152
Attorney Docket No.: FR920020060US1

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

In response to the Office Action of July 13, 2007, having a shortened statutory period for response set to expire on October 13, 2007, and finally rejecting all claims, Applicants respectfully submit this Appeal Brief.

(I) Real Party in Interest

The real party in interest for this Application is assignee INTERNATIONAL BUSINESS MACHINES CORPORATION of Armonk, NY.

(II). Related Appeals and Interferences

There are no related appeals or interferences.

(III). Status of Claims

Claims 1-10 and 12-14 are pending. Claims 1, 4-9, and 12-13 stand rejected under 35 USC 102 as being anticipated by US Publication Number 2003/0158816 for Rouse3. Claims 2-3, 10 and 14 stand rejected under 35 USC 103 (a) as being unpatentable over Rouse in view of US Publication Number 2002/0120763 for Miloushev et al. Claims 1-10 and 12-14 are being appealed.

(IV). Status of Amendments

Amendments to the claims filed on April 19, 2007 have been entered. No further amendments have been made to the claims.

(V). Summary of claimed subject matter

(V.A) Claim 1

Support for each element of independent claim 1 is indicated in plain brackets (). Claims 1 is directed to a method (Figs. 2, 3, 4, 5 and 6; page 4 lines 3-5) for providing a customer with access, through a network, to a media content file (page 4 lines 3-5, page 8 lines 18-31, page 11 lines 1-4). The method comprises opening a session with the customer computer (Fig. 4 step 420; page 11 lines 15-17) and receiving a request from

the customer computer to view a media content file (Fig. 2 step 200; Fig. 4 step 410; page 8 lines 19-25). A temporary metafile is created having a temporary metafile name (Fig. 4 step 430; Fig. 5 step 530; page 4 lines 8-9, page 8 lines 31-32, page 9 line 1, page 11 lines 23-24, page 13 lines 1-10). The temporary metafile contains a network address where the media content file can be obtained (Fig. 5 step 540; page 4 lines 8-9, page 9 lines 1-5, page 13 lines 17-19). The temporary metafile also contains an unencrypted file path leading to the media content file (Fig. 5 step 540; page 4 lines 9-11, page 12 lines 19-22, page 13 lines 17-19). The temporary metafile name is sent to the customer computer (Fig. 2 step 210; Fig. 4 step 440; Fig. 6 step 600; page 4 lines 11-12, page 8 lines 25-31, page 11 lines 23-24). The temporary metafile is canceled or deleted before or at the end of the session with the customer computer (Fig. 6 step 650; page 4 lines 12-14, page 15 lines 23-28).

(V.B) Claim 12

Support for each element of independent claim 12 is indicated in plain brackets (). Claim 12 is directed to an apparatus for providing a customer computer with access, through a network, to a media content file (page 4 lines 3-5, page 8 lines 18-31, page 9 lines 1-4). A server (100 in Figs. 1 and 2) for a computer system (90 in Fig. 1; page 7 lines 3-17) provides a customer computer with access, through a network, to a media content file (page 4 lines 3-5, page 8 lines 18-31, page 9 lines 1-4). The server comprises means for opening a session (150 in Fig. 1; page 8 lines 8-11), means for receiving from the customer computer a request to view a media content file (page 8 lines 11-16), means for creating a temporary metafile (Fig. 5 step 530; 150 in Fig. 1; page 13 lines 1-3) containing a network address where said media content file can be obtained and an encrypted file path leading to said media content file (Fig. 5 step 540; page 13 lines 17-19), means for sending the temporary metafile name to the customer computer (Fig. 5 step 540; page 13 lines 21-22), and means for canceling or deleting the metafile before or at the end of the session with the customer computer (Fig. 6 step 650; page 15 lines 23-28).

(V.C) Claim 13

Support for each element of independent claim 13 is indicated in plain brackets (). Claim 13 is directed to a program product (page 4 lines 3-5) for providing a customer with access, through a network, to a media content file (page 4 lines 3-5, page 8 lines 18-31, page 11 lines 1-4). The program product comprises program instructions to open a session with the customer computer (Fig. 4 step 420; page 11 lines 15-17) and receiving a request from the customer computer to view a media content file (Fig. 2 step 200; Fig. 4 step 410; page 8 lines 19-25). A temporary metafile is created by program instructions, the metafile having a temporary metafile name (Fig. 4 step 430; Fig. 5 step 530; page 4 lines 8-9, page 8 lines 31-32, page 9 line 1, page 11 lines 23-24, page 13 lines 1-10). The temporary metafile contains a network address where the media content file can be obtained (Fig. 5 step 540; page 4 lines 8-9, page 9 lines 1-5, page 13 lines 17-19). The temporary metafile also contains an unencrypted file path leading to the media content file (Fig. 5 step 540; page 4 lines 9-11, page 12 lines 19-22, page 13 lines 17-19). Program instructions send the temporary metafile name to the customer computer (Fig. 2 step 210; Fig. 4 step 440; Fig. 6 step 600; page 4 lines 11-12, page 8 lines 25-31, page 11 lines 23-24). Program instructions cancel or delete the temporary metafile before or at the end of the session with the customer computer (Fig. 6 step 650; page 4 lines 12-14, page 15 lines 23-28).

(V.D) Claim 2

Claim 2, which depends from claim 1 is directed to a method in which the temporary metafile also contains an encrypted name of the media content file (page 8 lines 31-32, page 9 lines 1-4 and 12-13, page 13 lines 17-19).

(V.E) Claims 3

Claim 3, which depends from claim 1 is directed to a process according to its parent claim and wherein the customer computer requests the temporary metafile to learn the encrypted media content file name, unencrypted media content file path and network address (page 9 line 10-13) and the customer computer subsequently sends the encrypted media content file name and the unencrypted media content file path to the network address of the media content file (page 9 lines 14-16).

(V.F) Claim 4

Claim 4, which depends from claim 1, is directed to a process according to its parent claim and wherein the creating step further comprises the step of computing said metafile name based on characteristics of said customer session (Page 9 lines 5-8).

(V.G) Claim 5

Claim 5, which depends from claim 1, is directed to a process according to its parent claim and wherein the customer session was opened with an application server, and further comprising the steps following executed by the customer computer (Fig. 2; Fig. 6, Page 14 lines 26-28): receiving the temporary metafile name (Fig. 2 step 210; page 8 lines 25-32, page 9 lines 1-4); using the temporary metafile name, requesting the temporary metafile from the application server (Fig. 2 step 215; page 9 lines 10-13); sending a request to the network address to receive and play the media content file identified by the encrypted media content file name and unencrypted media content file path (Fig. 2 step 220, page 9 lines 14-16) and receiving and playing the named media content file (page 9 lines 30-32).

(V.H) Structure for means plus function claim elements

Claim 12

The structure, material or acts described in the specification corresponding to each "means plus function" element are indicated in stylized brackets {}. The server

comprises: means for opening a session {100 and 150 in Fig. 1; page 8 lines 8-11}, means for receiving from the customer computer a request to view a media content file {page 8 lines 11-16}, means for creating a temporary metafile {150 in Fig 1; page 13 lines 1-3}, means for sending the temporary metafile name to the customer computer {page 13 lines 21-22}, and means for canceling or deleting the metafile before or at the end of the session with the customer computer {150 in Fig. 1; page 15 lines 23-28}.

(VI). Grounds of Rejection to be reviewed on appeal

Claims 1, 4-9, and 12-13 are rejected under 35 U.S.C. 102 as being anticipated by U.S. Publication No. 2003/0158816 (hereafter Rouse). Claims 2-3 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rouse in view of U.S. Publication No. 2002/0120763 (hereafter Miloushev).

The questions for appeal are whether or not claims 1, 4-9, and 12-13-14 are anticipated by Rouse under 35 U.S.C. 102, and whether or not claims 2-3 and 10 are obvious over Rouse in view of Miloushev.

(VII). Argument

(VII.A) Principles of Law

Anticipation

The Examiner must make a prima facia case of anticipation. "A person shall be entitled to a patent unless. . . (b) the invention was patented or described in a printed publication in this or a foreign country . . . more than one year prior to the date of the application for patent in the United States." 35 U.S.C. 102. It is settled law that each element of a claim must be expressly or inherently described in a single prior art reference to find the claim anticipated by the reference. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.3d 63, 631, 2USPQ2d 1051,1053 (Fed. Cir. 1987), cert. denied, 484 U.S. 827 (1987). Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1951 (Fed. Cir. 1999)(citations and internal quotation marks omitted). Claims interpretation begins with the plain meaning of the language of the claims themselves. "The words of the claims themselves define the scope of the invention, and are given their ordinary and customary meaning unless the patentee has chosen to use terms in some other manner." Allen Engineering Corp. v. Bartell Industries, 299 F.3d 1336, 1344, 63 USPQ2d 1769, 1772 (Fed. Cir. 2002).

Obviousness

Under 35 USC 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Graham v. John

Deere Co 383 US 1 (1966). When the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvous KSR Int'l Co. v. Teleflex Inc. 550 U.S. ___ (2007) citing nited States v. Adams 383 US 39, 0 (1966). A court must ask whether the improvement is more than the predictable use of prior art elements according to established functions. KSR Int'l Co/ v. Teleflex Inc. 550 U.S. ___ (2007).

(VII.B) Rejection of Claims 1, 13 under 35 USC 102 over US 2003/0158816 (Rouse)

Applicants have contended that claims 1 and 13, are allowable because they include features that are neither disclosed nor suggested by Rouse or any other references cited in the First Office Action, either individually or in combination.

(VII.B.1) "said metafile containing a network address where said media content file can be found and an unencrypted file path leading to said media content file"

Claims 1 and 13 include a first feature, "said metafile containing a network address where said media content file can be found and an unencrypted file path leading to said media content file."

As clearly provided in the specification, the temporary metafile comprises an unencrypted file path for the named media content file (page 9, lines 1-4). Moreover as further clearly provided, the path contains the address o the media content file (page 9 lines 4-5). Again, the specification clearly provides that the servlet writes into the metafile the path and the unencrypted address of the media content server (page 13 lines 17-19). Accordingly, consistent with the specification and the plain meaning of the claim language, the address and file path for the media content file are contained in the metafile.

The Examiner has implicitly conceded that the metafile of Rouse does not contain the address and file path of the media content file (Office Action of July 13, 2007,

paragraph 5). Instead, the metafile of Rouse contains a URL reference to a temporary subdirectory. The temporary subdirectory, in turn is associated with a redirect directive.

The Examiner, however, argues that this feature of claims 1 and 13 is contrary to its plain meaning. The Examiner's argument is that "said metafile containing a network address where said media content file can be found" does not mean that the address contained in the metafile is the address of the media content file. Instead, the Examiner suggests that this only means that the media content file can be obtained from the address in the metafile. Thus, the Examiner is arguing that "said metafile containing a network address where said media content can be found and an unencrypted file path leading to said media content file" is identical to "said metafile containing a network address of a temporary subdirectory where said media content file can be obtained by a redirect directive that leads to where said media content file can be found and an unencrypted file path leading to the temporary subdirectory with a redirect directive leading to said media content file".

As pointed out in paragraph VII.A, claims interpretation begins with the plain meaning of the language of the claims themselves. "The words of the claims themselves define the scope of the invention, and are given their ordinary and customary meaning unless the patentee has chosen to use terms in some other manner." Allen Engineering Corp. v. Bartell Industries, 299 F.3d 1336, 1344, 63 USPQ2d 1769, 1772 (Fed. Cir. 2002). Thus, in accordance with the ordinary and customary meaning of the term "where the media content file can be found", this feature of claims 1 and 13 means where the media content file is located.

Moreover, the address in Rouse is for a subdirectory that may lead to the media content file. As clearly provided in Rouse, the subdirectory is initially empty. Therefore, the subdirectory will not lead to the media content file until the redirect directive is associated with it. Thus, "an address where the media content file can be found" is not inherent in Rouse even if, arguendo, the claims of the present invention were not

interpreted to require the actual address of the media content file to be contained in the metafile.

The Examiner has failed to make a prima facia case that the element "said metafile containing a network address where said media content file can be found and an unencrypted file path leading to said media content file" is anticipated by Rouse.

***(VII.B.2)* "sending to the customer computer the temporary metafile name"**

Claims 1 and 13 include a second element "sending to the customer computer the temporary metafile name".

In the present application, the metafile itself is not immediately sent by the server to the customer computer. Instead, upon receipt of the request for protected media content, the present invention provides that only the metafile name is sent to the customer computer by the server (page 8 line 18 – page 9 line 8). The information in the metafile (namely, the network address where the media content file can be found and unencrypted file path) is retrieved by the customer computer (page 9 lines 10-12). This information is then used by the customer computer to access the media content file (page 9 lines 14-16).

In Rouse, a metafile is sent by the web server to a subscriber upon receipt of the request for protected media content (see step B in figs. 2 and 3; [0127 lines 8-14). In the Office Action of July 13, 2007, the Examiner mistakenly argues that this feature is disclosed in Rouse at [0116] lines 9-14 and at [0122} lines 1-9, and that the temporary metafile name is in the form of /station/access/tempname. However, Rouse provides that the temporary access subdirectory and not the metafile is of the form "station/access/tempname" ([116] lines 14-16). Moreover, the Examiner mistakenly argues that the metafile name is sent to the customer computer in Rouse. The text cited by the Examiner provides creation of a metafile with a URL reference to access a temporary access subdirectory and that the client player is allowed to connect to the ProtectURL through a separate and temporary link to the metafile. As specifically

pointed out above (see step B in figs. 2 and 3; [0127 lines 8-14), the metafile and not the metafile name is sent to the customer computer in Rouse.

The Examiner has failed to make a prima facia case of anticipation of the second element, "sending to the customer computer the temporary metafile name."

(VII.C) Rejection of Claim 12 under 35 USC 102 over US 2003/0158,816 (Rouse)

Applicants have contended that claim 12, as originally filed is allowable because it includes features that are neither disclosed nor suggested by Rouse or any other references cited in the First Office Action, either individually or in combination.

(VII.C.1) ***elements previously discussed under claim 1***

"said metafile containing a network address where said media content file can be found and an unencrypted file path leading to said media content file"

This element is directed to a server operating a program of instruction substantially similar to the first element argued under claims 1 and 13. These arguments will not be repeated here.

"means for sending to the customer computer the temporary metafile name"

This element is directed to a server operating a program of instruction substantially similar to the second element argued under claims 1 and 13. These arguments will not be repeated here.

(VII.D) Rejection of Claim 2 under 35 USC 103 over US 2003/0158,816 (Rouse) in view of US 2002/0120763 (Miloushev et al.)

Applicants have contended that claim 2, as originally filed is allowable independently of its parent claim 1, because it includes features that are neither disclosed

nor suggested by Rouse or any other references cited in the First Office Action, either individually or in combination.

(VII.D.1) "said temporary metafile also contains an encrypted name of said media content file."

Claim 2 includes the element "said temporary metafile also contains an encrypted name of said media content file." Rouse does not disclose or suggest a metafile containing an encrypted name of the media content file. Moreover, Rouse does not even disclose or suggest a metafile containing an unencrypted name of the media content file. The metafile of Rouse provides a URL reference to a subdirectory created by the subscriber client application. This is not an encrypted name of the media content file or even an unencrypted name of the media content file.

In the Office Action of July 13, 2007, the Examiner concluded in error that the temporary metafile of Rouse contains a media content file because it contains the redirect which contains the name of the media content file. However, the metafile of Rouse contains an address of a subdirectory. The subdirectory is appended with a redirect directive. Therefore, the Metafile of Rouse contains neither the media content file name or the redirect directive. Moreover, Rouse does not disclose or suggest that the metafile, the subdirectory, or the redirect contain the name of the media content file.

The office action suggests that it would have been obvious to modify Rouse by using encryption as taught by Miloushev. Applicants respectfully disagree. One of ordinary skill would have no reason to encrypt the media content file name in the system and method of Rouse because the filename is not provided in the metafile. As described above, Rouse employs a different method of protecting the media content.

Also, Miloushev does not disclose or suggest that a server encrypt a media content file name and provide the encrypted name to a customer (client) computer. Instead, Miloushev provides in [395] that the encryption key resides on the customer (enterprise's] premises.

Moreover, the Examiner has inappropriately modified Rouse by adding encryption of the media content file name. Rouse teaches away from encryption, stating that a new item in Rouse is "a means to protect live Content such as Webcasts without the use of encryption" ([0143] lines 3-4). Thus, it is inappropriate to modify Rouse contrary to the specific teaching of Rouse.

The Examiner has failed to demonstrate that the elements of claim 2 are no more than the predictable use of prior art elements according to established functions. The Examiner has not provided any prior art reference for the element "said temporary metafile also contains an encrypted name of said media content file." Moreover, the Examiner has not taken into account that Rouse teaches away from using encryption.

(VII.E) Rejection of Claim 3, under 35 USC 103 over US 2003/0158,816 (Rouse) in view of US 2002/0120763 (Miloushev et al.)

Applicants have contended that claim 3, is allowable independently of its parent claim 1, because it includes a feature that is neither disclosed nor suggested by Rouse or Miloushev, either individually or in combination.

(VII.E.1) "said customer computer requesting said temporary metafile to learn the encrypted media content file name, unencrypted media content file path and said network address, and said customer computer subsequently sending said encrypted media content file name and said encrypted media content file path to said network address"

Claim 3 includes the element "said customer computer requesting said temporary metafile to learn the encrypted media content file name, unencrypted media content file path and said network address, and said customer computer subsequently sending said encrypted media content file name and said encrypted media content file path to said network address." In an embodiment of the present invention, the customer computer requests the temporary metafile to learn the encrypted media content file name, file path

and address. This information is then sent by the customer computer to the address of the media content server to access the media content file.

Rouse does not disclose or suggest the customer computer requesting the temporary metafile, but rather the customer computer requests the media content file and is provided with the URL (address) of the temporary access subdirectory. Thus, in Rouse the customer computer does not learn the encrypted media content file name. In Rouse the customer computer must connect to the protected URL through the application server. The web address and file name of the protected media content file are not provided to the customer computer. In Rouse, the metafile contains a URL reference to access a subdirectory. Moreover, Rouse provides that the subdirectory is empty, but that it is associated with a temporary redirect directive. Miloushev does not provide what Rouse lacks.

Neither Rouse nor Miloushev disclose or suggest the customer computer sending the encrypted media content file name and the unencrypted file path to the media content server to access the media content file. Instead, in Rouse the customer computer requests media content and receives a metafile having a request URL where a temporary access subdirectory is located. The customer computer then connects to the temporary access subdirectory at the request URL and through a redirect directive is connected to the media content server. In Rouse the customer computer never receives the file path to the media content server, but only the address of the temporary access subdirectory. In fact, it is the invention of Rouse that the file path is hidden and a portion of it only exists in the temporary access subdirectory. Moreover, as described above, Rouse teaches away from an encrypted media content file name.

The Examiner has failed to demonstrate that the elements of claim 2 are no more than the predictable use of prior art elements according to established functions. The Examiner has not provided any prior art reference for the element "said customer computer requesting said temporary metafile to learn the encrypted media content file name, unencrypted media content file path and said network address, and said customer

computer subsequently sending said encrypted media content file name and said encrypted media content file path to said network address."

(VII.F) Rejection of Claim 4 under 35 USC 102 over US 2003/0158,816 (Rouse)

Applicants have contended that claim 4 is allowable independently of its parent claim 1, because it includes a feature that is neither disclosed nor suggested by Rouse or any other references, either individually or in combination.

(VII.F.1) "computing said metafile name based on characteristics of said customer session"

Claim 4 includes the element "computing said metafile name based on characteristics of said customer session". This is important because, computing the name of the metafile based on characteristics of the customer session, such as sessionID, provides a unique metafile name that can not be easily determined or anticipated by potential pirates and can only be used during the customer session (see specification page 9, lines 5-8), thus making the metafile name more secure.

In the office action of July 13, 2007, the Examiner suggests in error that this feature is provided by Rouse at [127].

> [0127] The entire connection process is initiated by a Client request for special Encoded Link created by a Dynamic Web Page Program. The link starts a process as a Filepushlink Overlay that creates an Encoded Metafile containing an encoded access directory name, ***creates the access directory name***, and appends a System File Redirect Directive entry all in response to the Client's request to start access to the Protected Content.

While this section of Rouse discloses creating an access directory name, it does not suggest creating a name for the metafile, or that any file name is based on characteristics of the customer session.

The Examiner has failed to make a prima facia case of anticipation of the element, "computing said metafile name based on characteristics of said customer session."

VII.G Rejection of Claim 5 under 35 USC 102 over US 2003/0158,816 (Rouse)

Applicants have contended that claim 4 is allowable independently of its parent claim 1, because it includes a feature that is neither disclosed nor suggested by Rouse or any other references, either individually or in combination.

(VII.G.1) "receiving said temporary metafile name" and "using said temporary metafile name, requesting the temporary metafile from said application server."

Claim 5 includes the elements "receiving said temporary metafile name" and "using said temporary metafile name, requesting the temporary metafile from said application server." As pointed out in the office action of July 13, 2007, paragraph 20, Rouse provides that the "web server sends webcast metafile back to subscriber (Fig. 2 event B: this event occurs in response to a request for a protected content ([0116] lines 1-5))." In the present invention, the server sends the metafile name (not the metafile) to the customer computer and the customer computer uses the metafile name to request the metafile. The step of the server sending the metafile name to the customer computer is neither disclosed nor suggested by Rouse, and the step of using the name to request the metafile is also absent in Rouse.

Sincerely,

Steven E. Bach
Reg. No. 46,530
Attorney for Applicants

(VIII) Claims Appendix

Listing of Claims:

1.(original) A method for providing a customer computer with access, through a network, to a media content file, said method comprising the steps of:

opening a session with the customer computer;

receiving from the customer computer a request to view a media content file;

creating a temporary metafile having a temporary metafile name, said metafile containing a network address where said media content file can be and an unencrypted file path leading to said media content file;

sending to the customer computer the temporary metafile name; and

canceling or deleting the metafile before or at the end of said session with the customer computer.

2. (original) The method of claim 1 wherein said temporary metafile also contains an encrypted name of said media content file.

3. (previously presented) The method of claim 2 further comprising the step of said customer computer requesting said temporary metafile to learn the encrypted media content file name, unencrypted media content file path and said network address, and said customer computer subsequently sending said encrypted media content file name and said unencrypted media content file path to said network address.

4. (original) The method of claim 1 wherein the creating step further comprises the step of computing said metafile name based on characteristics of said customer session.

5. (previously presented) The method of claim 4 wherein said customer session was opened with an application server, and further comprising the following steps executed by the customer computer:

receiving said temporary metafile name;

using said temporary metafile name, requesting the temporary metafile from said application server;

sending a request to said network address to receive and play said media content file identified by said encrypted media content file name and unencrypted media content file path; and

receiving and playing the named media content file from said network address.

6. (previously presented) The method of claim 1 further comprising the following steps performed by a media content server having said network address:

upon receipt of the unencrypted file path, checking if said unencrypted file path is a file path of an existing media content file accessible by the media content server, and if so, sending this media content file for playing to the customer computer.

7. (original) The method of claim 1 wherein said customer session is opened between said customer computer and an application server or a media content server.

8. (previously presented) The method of claim 1 further comprising the following step performed by the customer computer:

installing a media player program; said media player program being automatically activated upon reception of said temporary metafile name to:

request the named temporary metafile from an application server with which said session was opened;

send data, identifying said media content file, within said named temporary metafile to said network address; and

receive and play said media content file received from said network address.

9. (original) The method of claim 1 wherein said temporary metafile name is sent to said customer computer within an HTML page.

10. (original) The method as set forth in claim 2 further comprising the step of determining an unencrypted name of said media content file by a naming convention applicable to other unencrypted media content file names available from said network address.

11. (deleted)

12. (original) A server for providing a customer computer with access, through a network, to a media content file, said server comprising:

means for opening a session with the customer computer;

means for receiving from the customer computer a request to view a media content file;

means for creating a temporary metafile having a temporary metafile name, said metafile containing a network address where said media content file can be obtained and an encrypted file path leading to said media content file;

means for sending to the customer computer the temporary metafile name; and

means for canceling or deleting the metafile before or at the end of said session with the customer computer.

13. (previously presented) A computer program product for providing a customer computer with access, through a network, to a media content file, said computer program product comprising:

a computer readable medium;

first program instructions to open a session with the customer computer;

second program instructions to receive from the customer computer a request to view a media content file;

third program instructions to create a temporary metafile having a temporary metafile name, said metafile containing a network address where said media content file can be obtained and an encrypted file path leading to said media content file;

fourth program instructions to send to the customer computer the temporary metafile name; and

fifth program instructions to cancel or deleting the metafile before or at the end of said session with the customer computer; and wherein

said first, second, third, fourth and fifth program are recorded on said medium.

14. (previously presented) The method of claim 2 further comprising the following steps performed by a media content server having said network address:

upon receipt of the encrypted media content file name, checking if said encrypted media content file name is correctly encrypted, and if so, sending this media content file for playing to the customer computer.

(IX). Evidence appendix

No evidence is presented.

(X). Related proceedings appendix

There are no related proceedings.